A New Emergency-Handling Mechanism based on IEEE 802.15.4 for Health-Monitoring Applications

Jay Shree Ranjit[1], Subodh Pudasaini[1] and Seokjoo Shin[1]
[1]Department of Computer Engineering, Chosun University
Seosuk-dong, Gwangju 501-759 – S. Korea
[e-mail: jayshreeranjit@gmail.com, subodh@chosun.kr]
*Corresponding author: Seokjoo Shin
[e-mail: sjshin@chosun.ac.kr]

Received August 27, 2013; revised December 18, 2013; accepted January 14, 2014; published February 28, 2014

Abstract

The recent advances in wireless communication systems and semiconductor technologies are paving the way for new applications over wireless sensor networks. Health-monitoring application (HMA) is one such emerging technology that is focused on sensing and reporting human vital signs through the communication network comprising sensor devices in the vicinity of the human body. The sensed vital signs can be divided into two categories based on the importance and the frequency of occurrence: occasional emergency signs and regular normal signs. The occasional emergency signs are critical, so they have to be delivered by the specified deadlines, whereas the regular normal signs are non-critical and are only required to be delivered with best effort. Handling the occasional emergency sign is one of the most important attributes in HMA because a human life may depend on correct handling of the situation. That is why the underlying network protocol suite for HMA should ensure that the emergency signs will be reported in a timely manner. However, HMA based on IEEE 802.15.4 might not be able to do so owing to the lack of an appropriate emergency-handling mechanism. Hence, in this paper, we propose a new emergency-handling mechanism to reduce the emergency reporting delay in IEEE 802.15.4 through the modified superframe structure. A fraction of an inactive period is modified into three new periods called the emergency reporting period, emergency beacon period, and emergency transmission period, which are used opportunistically only for immediate emergency reporting and reliable data transmission. Extensive simulation is performed to evaluate the performance of the proposed scheme. The results reveal that the proposed scheme achieves improved latency and higher emergency packets delivery ratio compared with the conventional IEEE 802.15.4 MAC.

Keywords: Emergency handling, IEEE 802.15.4 MAC, health monitoring application

This study was supported by research fund from Chosun University, 2012

http://dx.doi.org/10.3837/tiis.2014.02.005

1. Introduction

With the advent of wireless networking systems and low-power embedded systems, boundless new possibilities have emerged for distributed system applications. The wireless sensor network (WSN) [1] is one such possibility that has been researched and implemented successfully for bridging the physical world and the digital information world through spatially distributed sensors and actuators. The WSN is not only implemented in larger geographical regions to monitor and transmit physical parameters such as temperature, sound, and pressure but has also been implemented for short-range communication between the devices around the personal workspace, which is known as the wireless personal area network (WPAN) [2]. Furthermore, it has been investigated for implementation in, or on, or around the human body, forming a wireless network for health-monitoring applications (HMA) [3]. In HMA, varieties of miniature and lightweight but powerful and intelligent sensing and communicating devices are deployed inside, on the surface, or around the human body that report sensed events such as heart rate, blood pressure, skin and body temperature, electrocardiogram, etc., to the center where the concerned health personnel can access this information.

The wireless network thus formed for HMA was initially focused on medical applications such as vital sign monitoring, but nowadays it covers a wider range of consumer electronics applications also such as sports, entertainment, personal authentication, and so on [4]. The medical applications, in general, report two types of vital sign information: regular normal signs (RNSs) and occasional emergency signs (OESs). The RNSs may include, but are not limited to, blood pressure, body temperature, and oxygen saturation level in the blood [5], whereas the OESs could be rapid fluctuation in ECG signals and reduced blood level in the brain. OESs should be urgently reported within the specified deadline in a reliable and real-time manner for immediate and accurate diagnoses because OESs are of critical importance, and if they are not addressed urgently, the consequences may be life threatening or result in permanent impairment of organ(s). On the other hand, RNSs are only required to be delivered with best effort.

Thus, it is necessary to design and engineer the overall protocol suite for HMA in such a way that it meets all the requirements with a special focus on reporting sensed life-threatening emergency events within the specified target delay. Different enhancements can be introduced in any of the protocol layers, from the transport layer to the physical layer, wherever it is deemed necessary. In this paper, we confine ourselves to the enhancements applicable to the Medium Access Control (MAC) sub-layer of the Data Link Layer.

Traditional MAC protocols are designed to maximize throughput, reduce latency, save energy, and ensure fairness, but these protocols lack an emergency-handling mechanism, which is one of the most important requirements of HMA. So, while designing MAC protocols for HMA, it must be ensured that the delay-sensitive data (emergency) are served within the application constraints. Low Rate Wireless Personal Area Network (LR-WPAN), IEEE 802.15.4 [6] standard, is widely used for HMA purposes owing to its features such as energy efficiency, scalability, and design flexibility. However, it cannot yet meet all the stringent network requirements for HMA because IEEE 802.15.4 does not have any emergency handling and traffic differentiation mechanisms. Consequently, IEEE 802.15.4 treats all data identically, and hence there is no mechanism for critical data to get higher priority during channel access.

Therefore, in this paper, we propose a new emergency-handling scheme with a modified IEEE 802.15.4 MAC frame structure to minimize the delay associated with reporting emergency events. The scheme allows opportunistic transmissions of emergency data during the inactive period. A fraction of the inactive period in the proposal is reframed into three new periods for emergency handling: the emergency reporting period (ERP), where the emergency devices can request for dedicated data transmission slots (DTSs) for reporting emergencies to the coordinator; the emergency beacon (EB) frame, which announces the DTSs' scheduling information for the emergency nodes that have successfully transmitted their requests to the coordinator; and the emergency transmission period (ETP), which consists of multiple DTSs for scheduled transmission of emergency data. These additional new periods are exclusively used for emergency-reporting purposes. If there is no emergency event, these periods act as inactive period such that the proposed protocol's behavior conforms completely to IEEE 802.15.4 MAC both structurally and functionally and hence makes it compatible with IEEE 802.15.4.

Recently, the IEEE 802.15.6 [7] standard for wireless body area networks (WBANs) with human-body-monitoring applications was released. The authors in [8], however, showed that for very small payloads IEEE 802.15.4 outperforms IEEE 802.15.6 in terms of the average packet loss ratio and average delay owing to the different channel access schemes applied to its MAC protocol as described in [6] and [7], respectively. Because the emergency traffic normally consists of small-payload-sized data [9], IEEE 802.15.4 has advantages in terms of network performance (especially for the delay constraint) over IEEE 802.15.6. That is why, in this paper, we focus on strengthening IEEE 802.15.4 for emergency handling.

The rest of the paper is organized as follows. Some of the related studies are presented and briefly discussed in Section 2. A brief overview of IEEE 802.15.4 MAC protocol is given in Section 3., The proposed scheme is explained in Section 4. Simulation results of the proposed scheme are discussed and compared with the conventional MAC scheme in Section 5, and the final section concludes the paper.

2. Related Work

Over the past decade, considerable efforts have been made to address the bounded time-delay emergency data in body sensor networks (BSNs) with HMA. Some remarkable results have been achieved [10–12] considering the QoS issues, mainly throughput and time delay performance assurance along with energy consumption and co-existence issues. Other researchers focused on designing a suitable MAC for HMA that fulfills all the HMA requirements. A number of MAC protocols have been researched and proposed for HMA, and most of these protocols are based on IEEE 802.15.4. Among these proposed protocols, the majority are focused on saving energy [13–16], while some are focused on QoS provisions [17–24]. Very few studies deal with the subject of emergency handling [23, 24].

Zhou et al. have developed BodyQoS with an admission controller, QoS scheduler, and virtual MAC on top of the real MAC for adaptively scheduling wireless resources at the time of channel degradation due to network loss, congestion, RF interference, etc., without having prior information on the underlying real MAC and ensuring adequate throughput for emergency data streams in HMA [10]. The real MAC follows polling-based access mechanism for channel access by the nodes and the aggregator. However, the use of individual polling-based access mechanisms by the aggregator causes inefficient channel utilization when reserving the maximum time for even a single packet transmission and incurs overhead due to the individual polling messages to each node. To overcome these drawbacks, Ren et al. have extended BodyQoS to BodyT2 with a group polling mechanism that supports QoS data [11]. Delay requirement is an additional issue along with throughput in BodyT2 and in the heterogeneous BSN. The test bed simulation results with different interference scenarios also report improved performance for BodyT2 compared to BodyQoS in terms of throughput, deadline adherence, and energy consumption.

Similarly, Li et al. have proposed communication energy modeling and optimization through joint packet size analysis for coexisting BSN and Wi-Fi networks that allows the BSN and Wi-Fi to dynamically change the packet's payload size based on their current delivery ratios [12]. The constraints used for optimization are throughput and time delay. In [10, 11], the proposed schemes rely on the QoS scheduler for controlled use of the channel such that the reservation requirements are attained at the expense of some scheduling delay, whereas the primary focus of [12] is on optimization in energy consumption issues for heterogeneous networks with BSN and Wi-Fi.

While considering IEEE 802.15.4, owing to the lack of a traffic prioritization mechanism, the critical data does not get any prioritized access in the medium, so emergency handling is not efficient in IEEE 802.15.4 MAC. Hence, many traffic differentiation schemes for prioritized data transmission have been suggested. Kim et al. have proposed a new service differentiation scheme based on the contention window (CW) size and backoff exponent (BE) [17]. In this scheme, higher-priority-class nodes have the lower CW and BE values than others. The scheme is applied during contention-based access period to support prioritized data transmission preemptively. However, because of the relatively long inactive period, the delay constraint for emergency traffic is not always guaranteed. Therefore, the scheme is not sufficient for handling emergency events for HMA.

Zhang and Dolmans have differentiated the traffic into two classes, periodic and bursty, and have proposed diversified contention-free periods (CFPs) for these two classes that are allocated based on the traffic arrivals in the previous superframe [18]. The contention access period (CAP) is also divided into two control channels: access channel1 (AC1) and access channel2 (AC2). However, the protocol is bound to suffer an unwanted delay due to the long CFPs. Also, the periodic traffic is not allowed to transmit in the CFP of bursty traffic and vice versa, so the delay bound is higher when different types of traffic occur at different CFPs.

Khaled et al. have classified traffic into two groups: critical and non-critical [19]. However, their study is mainly concentrated on determining the number of retransmissions based on traffic criticality, i.e., providing the maximum number of retransmissions to critical traffic, and avoids other QoS issues.

Kwak and Ullah have proposed a traffic-adaptive MAC for handling emergency and on-demand traffic, in which a table is maintained to store the traffic patterns of the nodes [20]. The protocol has a superframe structure that resembles the conventional IEEE 802.15.4 MAC with a configurable contention access period (CCAP) and CFP. So, this MAC is bound to incur undesirable delays because of the inefficient superframe structure for delay-sensitive traffic.

Yun et al. have proposed the on-demand MAC that dynamically reconfigures the superframe structure (varies the beacon interval) during run time according to the bandwidth request from sensor nodes, supporting real-time transmission [21]. They have classified the traffic as real-time message (RTM) and non-real-time message (NRTM). An RTM is delivered by reserving a guaranteed transmission slot (GTS), whereas an NRTM requires CAP slots for data transmission. For the same reason, RTM transmission in the GTS slots incurs additional delay.

Li and Tan have proposed an ultra-low-power MAC that determines the access priority of the nodes based on the energy constraint and data time criticality in order to vary the beacon interval [22]. The nodes with the highest medium access priority are given the capability to change the beacon interval. However, the basic superframe structure of the protocol is similar to the IEEE 802.15.4 superframe that provides a long inactive period after the CFP, and hence the scheme is inefficient for reporting emergency events occurring in the CFP.

Some other studies focus on explicit resource allocation for emergency handling. Lee C., Lee H.S., and Choi have proposed an enhanced MAC protocol of IEEE 802.15.4 for HMA with an enhanced superframe structure containing an emergency slot (ES) for emergency handling [23]. The ES is a short period where data transmission is described by "success" or "fail." The superframe contains a long CFP followed by an inactive period. Therefore, an emergency occurring in the CFP incurs an unnecessary delay due to the lengthy inactive period. Otgonchimeg and Kwon have proposed an emergency-handling MAC protocol for human body communication using emergency GTS (EGTS) in the CFP [24]. Emergency events are treated as regular events, and the number of EGTSs required to handle possible emergencies is calculated. The channel access mechanism in EGTS is Slotted ALOHA. Problems may arise in the protocol when multiple emergencies occur. In addition, in a real-life scenario, the emergency events are unpredictable, occasional events, and allocating resources solely for those events decreases the bandwidth utilization.

Apart from the emergency-handling schemes for HMA, we introduce an opportunistic emergency-handling MAC scheme that strengthens IEEE 802.15.4 MAC by reducing the emergency-reporting delay in HMA, thereby providing a reliable data transmission method for emergency events.

3. IEEE 802.15.4 MAC Overview

The IEEE 802.15.4 standard defines the physical layer and the MAC sub-layer specifications for LR-WPAN. The physical layer specifies three operating frequency bands, i.e., an 868 MHz band with a single channel, a 915 MHz band with 10 channels, and a 2.4 GHz band with 16 channels. The available data rates vary from 20 kbps to 250 kbps depending on the frequency band.

The MAC layer specifies two operational modes: non-beacon mode and beacon-enabled mode. The selection of the operational mode is decided by the personal address network coordinator (PANC). Contention-based un-slotted carrier sense multiple access/collision avoidance (CSMA/CA) is used in the non-beacon mode, whereas a hybrid access mechanism (consisting of contention-based slotted CSMA/CA and optional contention-free time division multiple access) is used in the beacon-enabled mode. The contention-free access mechanism in the beacon-enabled mode is specified to allocate conflict-free GTSs for transmitting time-critical data, whereas there is no such GTS mechanism in the non-beacon mode. Because the GTS mechanism is likely to support reliable transmission of emergency data, the beacon-enabled mode is analyzed in this paper from the emergency-handling perspective.

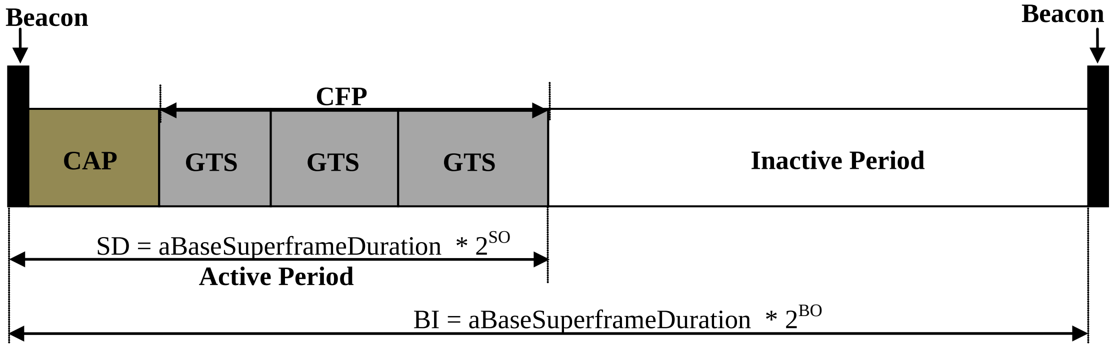

Fig. 1. IEEE 802.15.4 superframe structure

The beacon-enabled mode imposes the use of a superframe structure as shown in **Fig. 1** [6], which is delimited by the two consecutive beacons. The duration between every two consecutive beacons gives the length of the superframe and is known as the beacon interval (BI). The BI is divided into two parts: an active period and an inactive period. The active period is also called the superframe duration (SD), which is the only portion of the BI where frame transmissions between a PANC and devices occur. The rest of the BI is the inactive period, where a PANC and devices enter the low-power mode. The structure of the superframe is defined by two parameters, the BO and the SO, each of which determines the length of the BI and the SD, respectively. These durations can be expressed as

$$BI = aBaseSuperframeDuration * 2^{BO} \quad (1)$$
$$SD = aBaseSuperframeDuration * 2^{SO} \quad (2)$$

and

$$InactivePeriod = BI - SD \quad (3)$$

where $0 \leq SO \leq BO \leq 14$ and the aBaseSuperframeDuration is 960 symbols[1] in the standard [6].

The active period comprises the beacon period, the CAP, and the CFP. Every superframe starts with a beacon issued by the coordinator that contains information related to the superframe specifications (such as the BO, the SO, duration of other fields that follow a beacon, GTS allocation schedule, etc.). The beacon is then followed by the mandatory CAP and an optional CFP. The CFP is activated once the resource request (GTS request) from a node to the PANC is received and approved.[2]

4. Proposed MAC Protocol

4.1 System Model and Assumptions

The proposed scheme is based on the IEEE 820.15.4 MAC standard, operating in the 2.4 GHz RF band with a star topology as shown in **Fig. 2**. The model consists of a central coordinating full functional device called the network coordinator (NC) and many other reduced functional

[1] One symbol duration is 16 μs.
[2] A GTS request is approved if it satisfies the conditions that upon allocation, the number of GTSs allocated does not exceed the maximum number of GTSs (i.e., 7).

devices known as sensing nodes (SNs). The NC can perform some enhanced functions such as synchronization with other surrounding SNs, slot allocation for SNs, and exchanging control packets. On the other hand, an SN only senses and transmits the sensed data to the NC. SNs can directly communicate with NC in a single-hop communication architecture. SNs can be wearable or implanted devices, whereas the NC also can be attached to the body or a remote place within the communication range of the SNs. Generally, the SNs are energy constrained because they are battery powered.

There are two types of messages issued by SNs: RNSs and OESs as described in Section 1. Besides these, SNs also transmit control frames such as association requests, GTS requests, and DTS requests.

The NC can process data received from the SNs and then send it to the monitoring station or server through other networks (i.e., cellular, WLAN, or wired). The other communication paradigm is beyond the scope of this paper.

There could be different independent HMAs where the corresponding NCs are connected to the monitoring station, e.g., one HMA per patient in a hospital room.

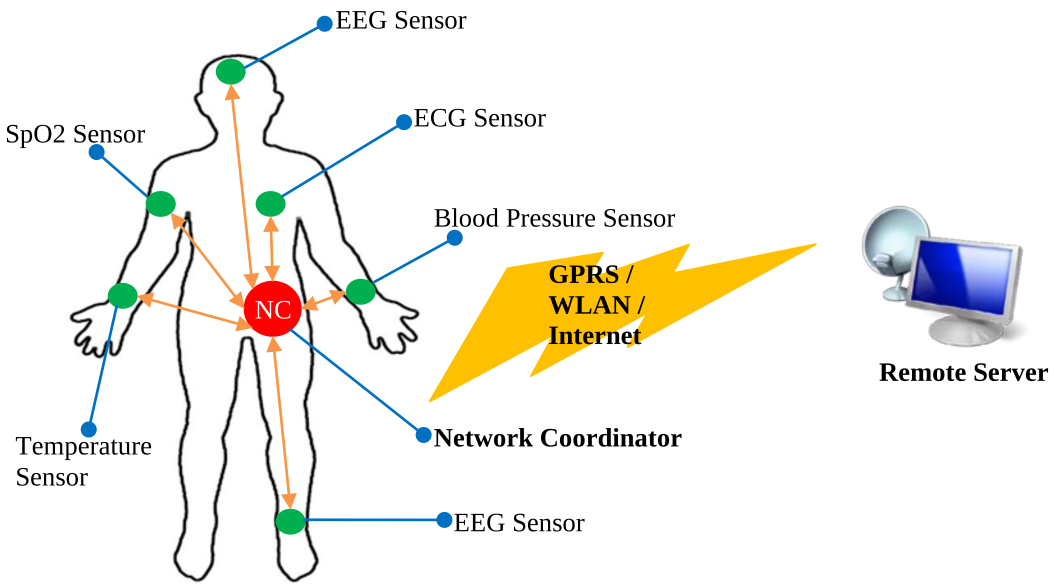

Fig. 2. Network model.

4.2 Modified Superframe Structure

The proposed scheme modifies the inactive period of the conventional superframe structure by inserting three new periods, as shown in **Fig. 3,** to handle emergency events.

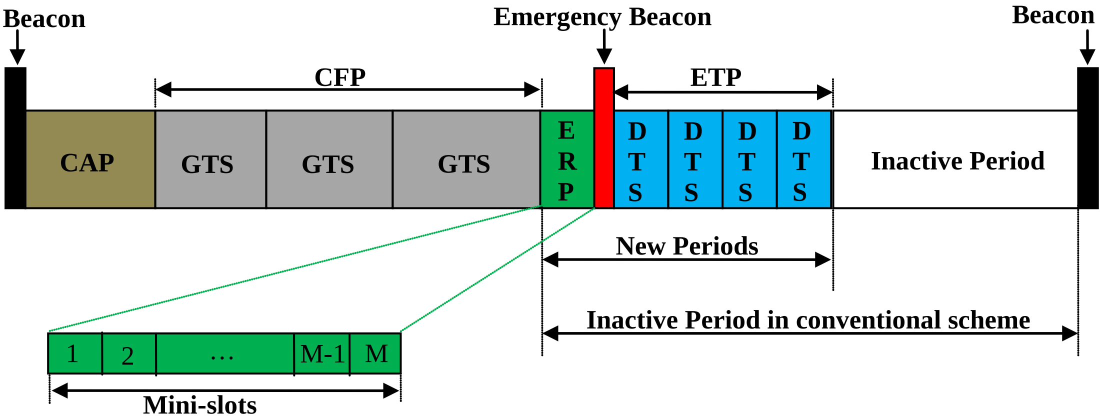

Fig. 3. Modified superframe structure**.**

Emergency Reporting Period (ERP): The ERP is a mandatory period in the proposed modified IEEE 802.15.4 scheme. It starts immediately after the CFP and ends before the beginning of the emergency beacon, if it exists. Otherwise, the ERP ends at the beginning of the inactive period of the superframe. In order to communicate this ERP information to all the SNs, the conventional beacon is modified to incorporate the additional fields ERP Start Time and ERP Length as shown in **Fig. 4**. The ERP is divided into M virtual mini-slots where SNs send a Dedicated Transmit Slot Request Command Frame (DTSRCF) to the NC by a random-backoff-based channel access mechanism for reporting any emergency events. The value of M is a design parameter that normally depends on the application type. For example, in a collapsing patient, the number of emergencies occurring is larger than usual so that the value of M must be greater, in order to handle all possible emergencies. For our proposed scheme, in order to maintain consistency with the conventional IEEE 802.15.4 superframe structure, we set the value of M equal to 7, which in turn makes the maximum number of DTSs allowed for an instance also equal to 7, similar to the maximum number of allowed GTSs in the conventional IEEE 802.15.4 MAC.

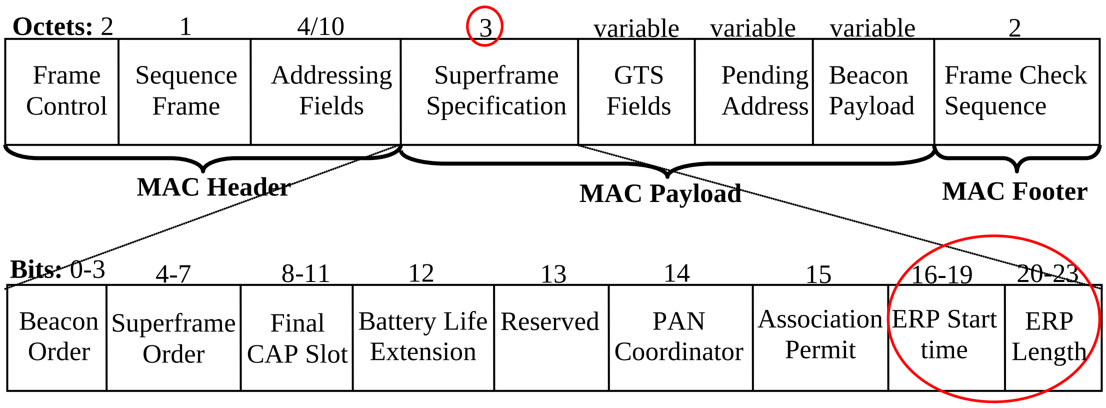

Fig. 4. Modified beacon frame structure in the proposed scheme.

A DTSRCF format is shown in **Fig. 5**, which consists of 2 bytes of Frame Control, 1 byte of Sequence Frame, 4 bytes of Addressing Fields, 1 byte Command Frame Identifier, and 1 byte of DTS Characteristics. The DTS Characteristics field further comprises 4 bits of a DTS Length field that contains the number of superframe slots being requested for the DTS, 1 bit of a DTS Direction field that is set to 1 to show the frame transmission from the SN to the NC, 1 bit of Characteristics Type that is set 1 for DTS allocation and 0 for DTS deallocation, and 2 bits of a Reserved field. The rest of the fields are as in the IEEE 802.15.4 standard [6].

Octets: 2	1	4	1	1
Frame Control	Sequence Frame	Addressing Fields	Command Frame Identifier	DTS Characteristics

Fig. 5. DTS request command frame format.

Emergency Beacon (EB): The EB starts immediately after the ERP. However, the EB is broadcasted by the NC only if any emergency is reported during the ERP, otherwise the EB period is treated as an inactive period. All SNs who have reported an emergency in the ERP should listen to the EB to check whether their reporting in the ERP is acknowledged by the NC. As shown in **Fig. 6,** the EB consists of 2 bytes of Frame Control, 1 byte of Sequence Frame, 4 bytes of Addressing Fields, variable bytes of the DTS Specification field, and 2 bytes of the Frame Check Sequence field. The DTS Specification field acknowledges all the requests acquired from the ERP mini-slots in the bitmap manner, so that the total number of bits is M in accordance with the size of the ERP mini-slots.

Octets: 2	1	4	variable	2
Frame Control	Sequence Frame	Addressing Fields	DTS specification	Frame Check Sequence

Fig. 6. Emergency beacon frame structure.

Emergency Transmission Period (ETP): The ETP starts just after the EB. The ETP is divided into a number of scheduled time slots called DTSs. Data transmission in the ETP follows the contention-free method. All the DTSs allocated by the NC are located in the ETP and occupy contiguous slots. The ETP may therefore grow or shrink depending on the number of successful requests obtained in the ERP. The maximum number of such DTSs allocated for an instance in a superframe is equal to M (i.e., the total number of mini-slots in the ERP).

4.3 Principle of Operation

In the proposed scheme, as shown in **Fig. 7**, if an SN detects an emergency event during the CFP, it waits until the start of the ERP. At the beginning of the ERP, the SN randomly selects a backoff value within [0, M]. If the backoff value is equal to 0, the SN immediately sends the DTSRCF, otherwise it keeps on decreasing the backoff value by 1 until it reaches zero at every completion of a mini-slot duration. Once the backoff value reaches 0, the DTSRCF is sent to the NC. After sending the DTSRCF, the SN waits for the emergency beacon. If the DTS is allocated to the SN in the emergency beacon, it waits for the corresponding DTS start time and then transmits its emergency data in that DTS. On the other hand, if it does not receive any DTS allocation information, the SN waits until the next CAP for data transmission on a contention basis.

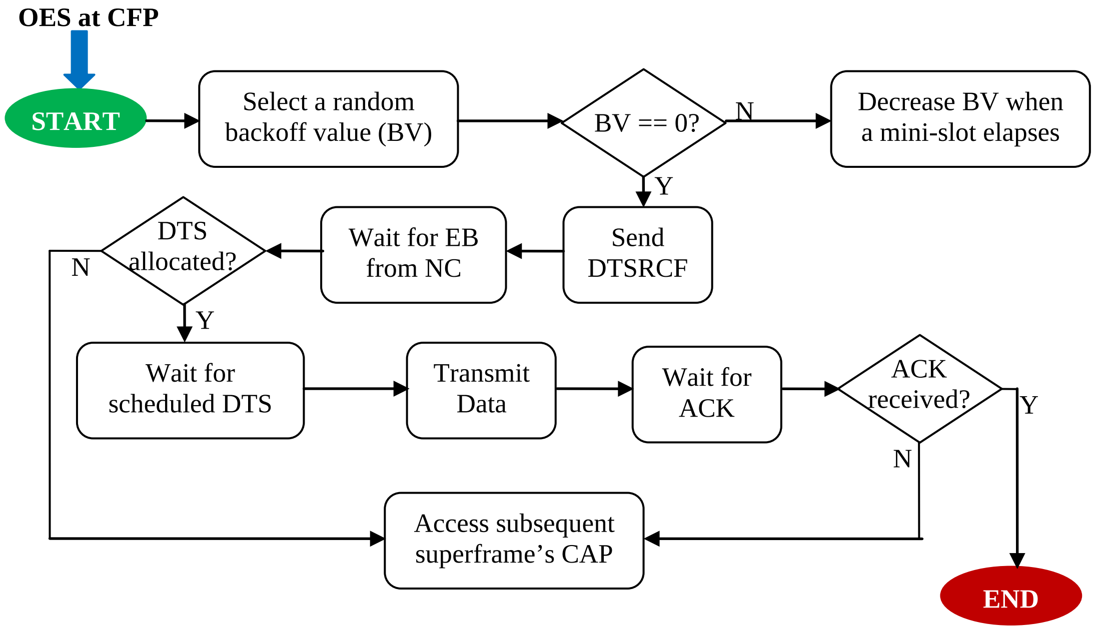

Fig. 7. Flow diagram of the proposed scheme.

Because OES traffic is transmitted only in the scheduled DTS, collisions do not occur during the OES traffic transmission. However, collisions may occur in the ERP mini-slots during the transmission of the DTSRCF. So, to reduce the collision probability during the ERP, the transmission of the DTSRCF is controlled by a random-backoff-based contention access method.

5. Simulation Results and Discussion

5.1 Simulation Environment

In order to evaluate protocol performance, we conducted a simulation of the proposed scheme on Castalia-3.2 [25], a discrete event network simulator specifically designed for sensor and body area networks based on the OMNeT++ platform [26]. Castalia supports the advanced channel model based on empirically measured data that defines a map of path loss. The modelt is not simply the connections between nodes but a complex model for temporal variation of path loss having mobility of nodes and interference based on received signal strength, etc. The simulation was carried out with a star topology as shown in **Fig. 2**, with the single-hop communication between the NC and the SNs.

The traffic is generated using the Poisson distribution with varying mean inter-arrival times (T_{mean}). The generated packet length is fixed at 40 bytes. The type of traffic is classified as OES or RNS. The ratio of OES to RNS in the simulation is x to $(1 - x)$. The value of x is varied from 1% to 5%.

The detailed simulation parameters and their values for IEEE 802.15.4 MAC from Castalia-3.2 [25] are summarized in Table 1.

Table 1. Simulation parameters and values

Simulation time	50 s		
Frequency band	2.4 GHz		
Data rate	250 kbps		
MAC Buffer Size	60 packets		
Frame Parameters	**Command Frames Information**	Association Request	8 bytes
		GTS Request	
		DTS Request	
	ACK Packet Size	6 bytes	
	Inter-Frame Spacing	SIFS	12 symbols
		LIFS	40 symbols
	Turnaround Time	12 symbols	
Superframe Parameters	**Beacon Order (BO)**	4	
	Superframe Order (SO)	3	
	aNumSuperframeSlots	16	
	aBaseSlotDuration	60 symbols	
	Beacon Information	Base Beacon Packet Size	12 bytes
		GTS Descriptor Size	3 bytes
	CAP Parameters	aMinCAPLength	440 symbols
		unitBackoffPeriod	20 symbols
		macMinBE	5
		macMaxBE	7
		macMaxCSMABackoffs	4
	CFP Parameters	Max. No. of GTS	7
	ERP Parameters	No. of Minislots (M)	7
	Emergency Beacon (EB) Information	Base EB Packet Size	9 bytes
		DTS Descriptor Size	3 bytes
	ETP Parameters	Max. No. of DTS	7

5.2 Performance Metrics

The performance of a system or a technology is usually characterized with the help of several metrics. In this subsection, we discuss the selected metrics that are suitable for the evaluation of IEEE 802.15.4 under the given reference scenario, to verify the need and usefulness of the proposed solution.

5.2.1 Delay

Delay is defined by the time required to transmit a packet of data from the source to the destination and is relevant only to the successfully transmitted packets. In this paper, delay is calculated by measuring the time interval from the instant a packet is available in the buffer for transmission until the ACK is received for that packet. The OES (or RNS) delay is the average delay, where all the delays of the successfully transmitted OES (or RNS) packets are accumulated and divided by the total number of received OES (or RNS) packets. Similarly, the overall delay is defined as the sum of all the delays from OES and RNS packets divided by the sum of the total number of successfully transmitted packets.

5.2.2 Packet Delivery Ratio (PDR)

The packet delivery ratio (PDR) is calculated by accumulating the total number of successfully received packets by the coordinator and the total number of packets generated at each node. It is an important characterization of wireless systems because it indicates whether a network is congested or not (e.g., a low delivery ratio implies that some data packets were lost). The number of dropped packets and retransmissions influence the PDR directly. The PDR is calculated as follows:

$$PDR = \frac{\text{Total number of succeffully transmitted packets to NC}}{\text{Total number of generated packets}} \tag{4}$$

In this paper, the PDR of the proposed scheme is calculated for OES traffic only and compared with that of the conventional IEEE 802.15.4 MAC.

5.3 Simulation Results and Discussions

In this section, we compare the simulated results of the proposed scheme with the conventional IEEE 802.15.4 MAC. The comparisons are made on the basis of the metrics defined in Section 5.2.

5.3.1 Delay Analysis

Figs. 8 to **11** show the comparisons between proposed scheme and conventional IEEE 802.15.4 in terms of packet delay. In general, packet delay increases as the number of nodes increases for both schemes. However, the proposed scheme has a lower packet delay than the conventional one.

Fig. 8(a) and **Fig. 8(b)** compare the OES traffic delays for the proposed and the conventional schemes when the packet inter-arrival rate is 1 s and the OES traffics percentage is varied (1% and 5%), respectively. In both cases, it is noted that the OES traffic delay is significantly reduced in the proposed scheme compared to the conventional IEEE 802.15.4 MAC. Delay is minimized by an average of 28% in the proposed scheme. In the graphs, when the number of nodes is 16 and 32, the delay is reduced drastically for the proposed scheme while it is reduced marginally when the number of nodes is equal to 4 and 8. For a low number of nodes, there are sufficient resources in both schemes for the OES nodes, so that there is not much difference between the two schemes.

The RNS delay is also reduced in the proposed scheme to some extent as seen in **Fig. 8(c)** and **Fig. 8(d).** That is because the fast transmission of the OES traffic increases the opportunity for the RNS traffic to be transmitted in the proposed scheme.

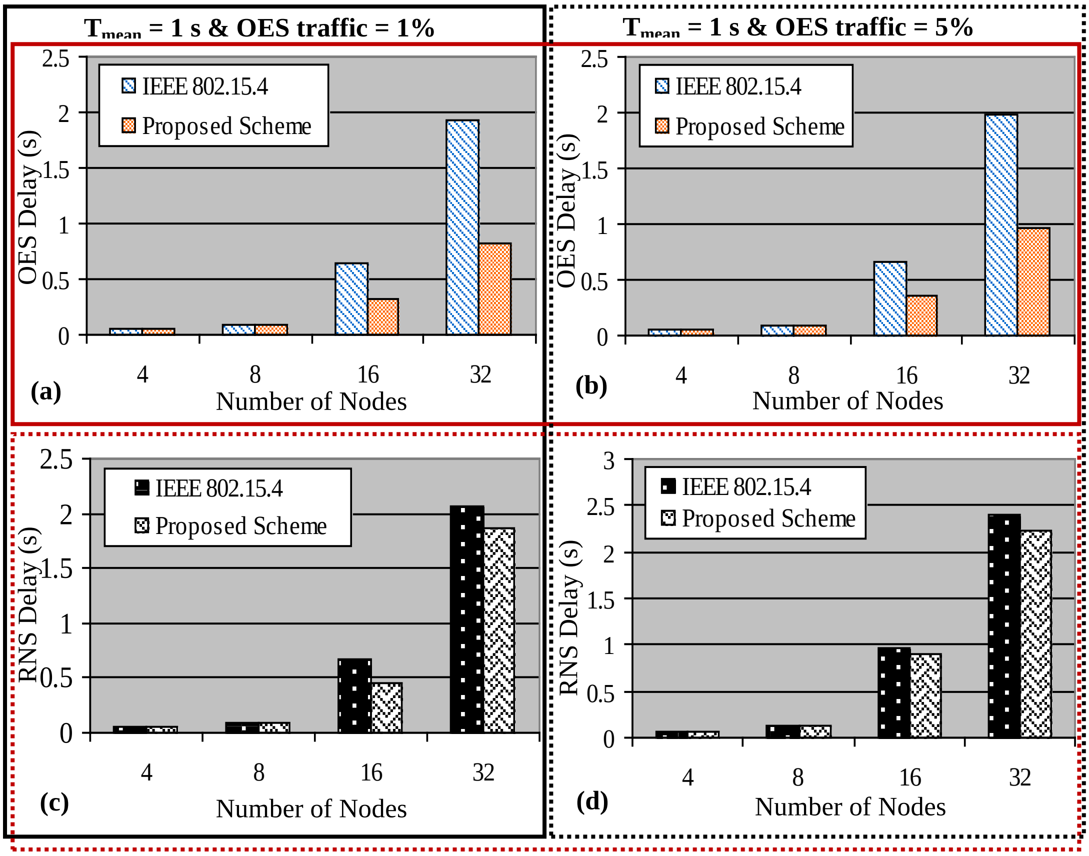

Fig. 8. OES and RNS delay comparison of proposed and conventional schemes when T_{mean} = 1 s and x = 1% and 5%.

Fig. 9 compares the overall traffic delay where the individual delays of both the OES and RNS traffic are summed up and divided by the sum of the total number of successful OES and RNS traffic. It is obvious that owing to the combined effects of the minimized OES and RNS delays in the proposed scheme, the overall delay is also lower in the proposed scheme than in the conventional IEEE 802.15.4 MAC.

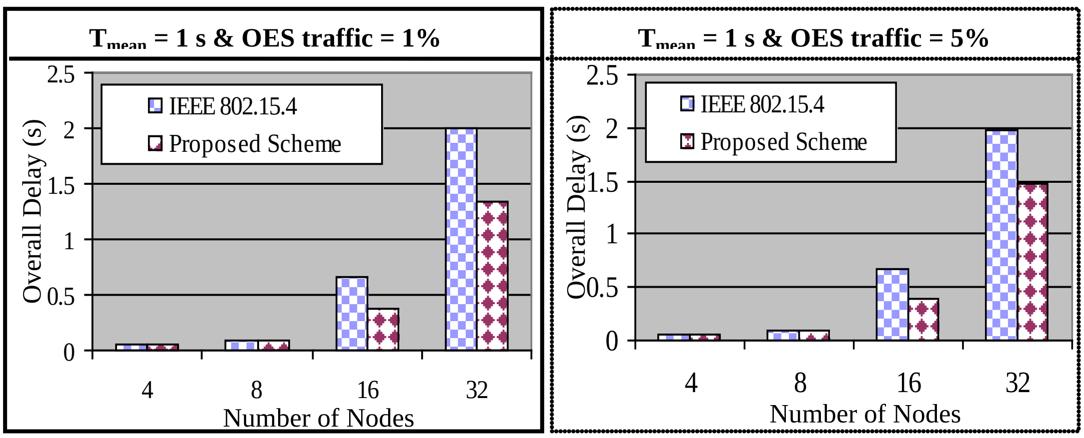

Fig. 9. Overall delay comparison of proposed and conventional schemes when T_{mean} = 1 s and x = 1% and 5%.

Fig. 10 compares the OES traffic delay and the RNS traffic delay when the packet inter-arrival rate is halved (0.5 s) compared to the previous figures. Similar to the previous figures, the OES delays are reduced sharply, and RNS delays are also marginally reduced. However, the delay increases in both the proposed and conventional schemes when the packet inter-arrival time shortens. Because a short traffic inter-arrival time means a speedier arrival of packets from the upper layer resulting in more congestion in the network, the delay is observed to be higher in both the schemes. However, the proposed scheme exhibits approximately 25% less OES traffic delay than the conventional scheme.

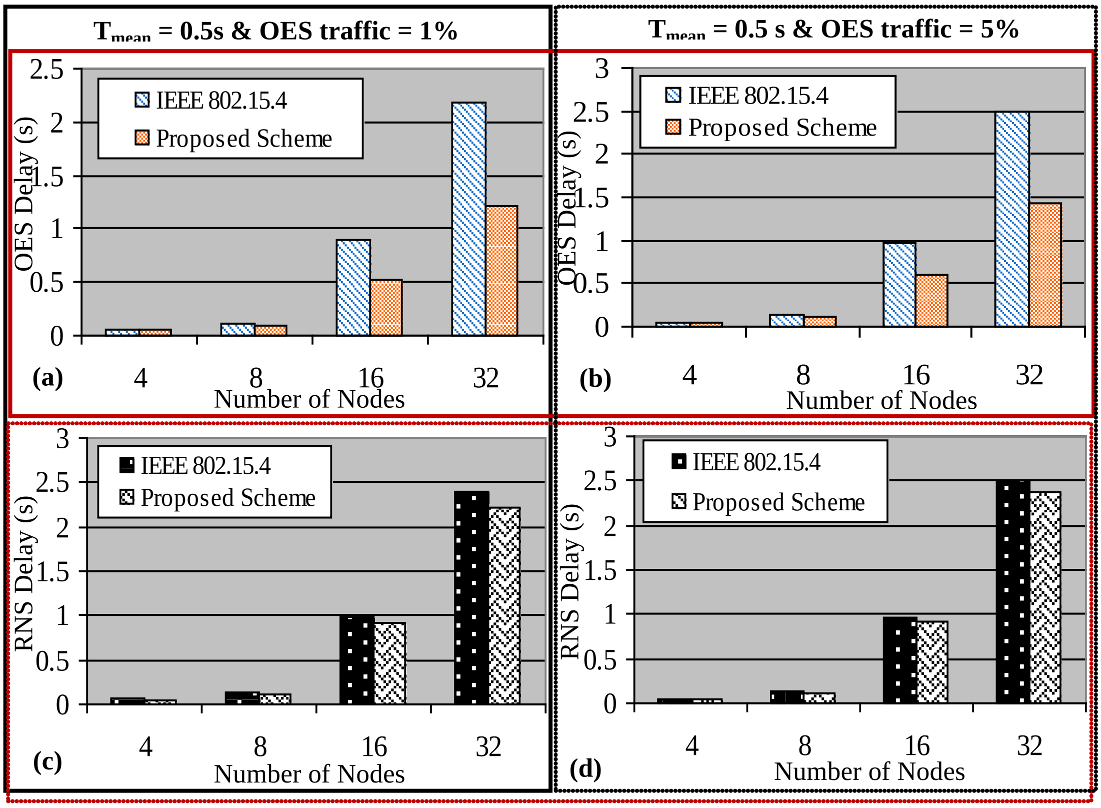

Fig. 10. OES and RNS delay comparison of proposed and conventional schemes when T_{mean} = 0.5 s and x = 1% and 5%.

Similar to the description for **Fig. 9**, the overall delay in **Fig. 11** is also lower in the proposed scheme than in the conventional MAC scheme.

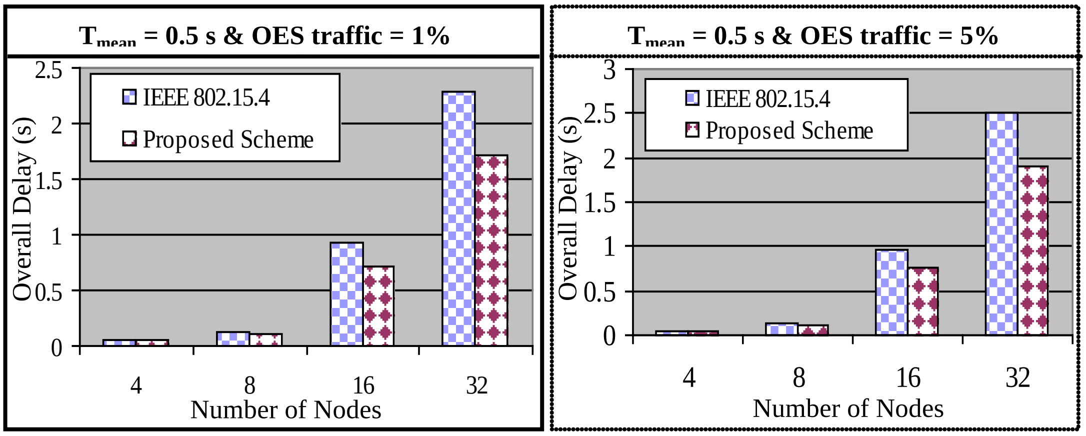

Fig. 11. Overall delay comparison of proposed and conventional schemes when T_{mean} = 0.5 s and x = 1% and 5%.

5.3.2 PDR Analysis

Fig. 12 shows a comparison of the PDR of OES traffic when the packet inter-arrival time is set to 1 s, and the OES traffic percentage varies from 1% to 5%. In general, the PDR decreases as the number of nodes increases in the both the conventional and proposed schemes. However, the decrease is very sharp in the conventional scheme, whereas it is gradual in the proposed scheme. Note that approximately 80% of the total generated OES traffic is successfully transmitted in the proposed scheme. This signifies that the proposed scheme is much more reliable than the conventional scheme for handling emergency traffic. There are some packet losses in the system for both schemes, which is due to events such as the limited MAC buffer size and the limited number of allowed retransmissions. In the simulation, these values are set to 60 packets, and 2, respectively.

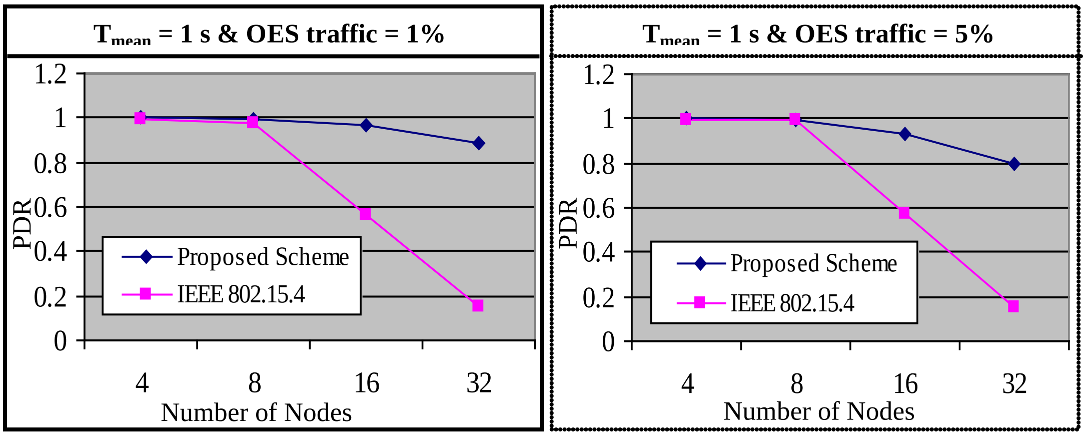

Fig. 12. PDR comparison of OES traffic of proposed and conventional schemes when T_{mean} = 1 s and x = 1% and 5%.

6. Conclusion and Future Studies

A new efficient emergency-handling scheme to enhance IEEE 802.15.4 considering HMA is presented in this paper. The scheme involved a modified IEEE 802.15.4 frame structure that opportunistically uses the inactive period for handling emergency events. An approximately 28% performance improvement over conventional IEEE 802.15.4 MAC for the reporting delay in emergency events is achieved through the proposed scheme. Similarly, a higher packet delivery ratio (more than 80%) for emergency traffic is also obtained in the proposed scheme. A marginal decrease in the delay in transmitting normal medical traffic is also achieved in the proposed scheme. Despite some energy issues due to the additional emergency beacon, the proposed scheme is more suitable for HMA thanks to its efficient emergency-handling capability and increased packet delivery ratio. Moreover, because of its simplicity, the proposed scheme can easily be adopted in IEEE 802.15.4 MAC for the efficient handling of emergency events.

Because this study is primarily focused on minimizing the emergency-reporting delay, other network issues are not addressed in detail. Energy efficiency and security are such issues that require more attention. Therefore, in future, this scheme can be evaluated and investigated on the basis of these issues. At the same time, the proposed scheme can be enhanced by applying priority-based access mechanisms in the already existing periods in the conventional IEEE 802.15.4 MAC.

References

[1] C. S. Raghavendra, K. M. Sivalingam and T. Znati, "Wireless Sensor Networks," Kluwer Academic Pub, 2004. Article (CrossRef Link)

[2] T. M. Siep, I.C. Gifford, R.C. Braley and R.F. Heile, "Paving the Way for Personal Area Network standards: An Overview of the IEEE P802.15 Working Group for Wireless Personal Area Networks," *Personal Communications*, vol.7, no. 1, pp. 37-43, February, 2000. Article (CrossRef Link)

[3] A. Milenkovic, C. Otto and E. Jovanov, "Wireless Sensor Networks for Personal Health Monitoring: Issues and Implementation," *Computer Communications*, vol. 29, no. 13, pp. 2521-2533, August, 2006. Article (CrossRef Link)

[4] M. Chen, S. Gonzalez, A. Vasilakos, H Cao and V. C. Leung, "Body Area Networks: A Survey," *Mobile Networks and Applications*, vol. 16, no. 2, pp. 171-193, April, 2011. Article (CrossRef Link)

[5] M.R. Yuce and C.K. Ho, "Implementation of Body Area Networks based on MICS/WMTS Medical Bands for Healthcare Systems," in *Proc. of 30th Annual International Conference of Engineering in Medicine and Biology Society (EMBS2008)*, pp. 3417-3421, August, 2008. Article (CrossRef Link)

[6] IEEE Std. 802.15.4-2006, Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), 2006. Article (CrossRef Link)

[7] IEEE Std. 802.15.6-2012, Part 15: Wireless Body Area Networks, 2012. Article (CrossRef Link)

[8] F. Martelli, C. Buratti and R. Verdone, "On the Performance of an IEEE 802.15.6 Wireless Body Area Network," in *Proc. of 11th European Wireless Conference-Sustainable Wireless Technologies (European Wireless)*, April, 2011.

[9] H. Chen, W. Wu and J. Lee, "A WBAN-based Real-time Electroencephalogram Monitoring System: Design and Implementation," *Journal of Medical Systems*, vol. 34, no. 3, pp. 303-311, March, 2009. Article (CrossRef Link)

[10] G. Zhou, J. Lu, C.Y. Wan, M.D. Yarvis and J.A. Stankovic, "BodyQoS: Adaptive and Radio Agnostic QoS for Body Sensor Networks," in *Proc. of 27th IEEE Conference on Computer Communications (INFOCOM 2008)*, April, 2008. Article (CrossRef Link)
[11] Z. Ren, G. Zhou, A. Pyles, M. Keally, W. Mao and H. Wang, "BodyT2: Throughout and Time Delay Performance Assurance for Heterogeneous BSNs," in *Proc. of INFOCOM*, pp. 2750-2758, April, 2011. Article (CrossRef Link)
[12] Y. Li, X. Qi, M. Keally, Z. Ren, G. Zhou, D. Xiao and S. Deng, "Communication Energy Modeling and Optimization through Joint Packet Size Analysis of BSN and WiFi Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 9, pp. 1741-1751, September, 2012. Article (CrossRef Link)
[13] G. Fang and E. Dutkiewicz, "BodyMAC: Energy Efficient TDMA-based MAC Protocol for Wireless Body Area Networks," in *Proc. of 9th International Symposium on Communications and Information Technology (ISCIT 2009)*, pp. 455-1459, September, 2009. Article (CrossRef Link)
[14] O. Begonya, A. Luis and V. Christos, "Design and Analysis of an Energy-Saving Distributed MAC Mechanism for Wireless Body Sensor Networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, no. 1, pp. 1-13, August, 2010. Article (CrossRef Link)
[15] M.A.I. Ameen, N. Ullah, M.S. Choudhary, S.M.R. Islam and K.S. Kwak, "A power efficient MAC Protocol for Wireless Body Area Networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1, pp. 1-17, February, 2012. Article (CrossRef Link)
[16] S.J. Marinkovic, E.M. Popovici, C. Soagnol, S. Faul and W.P. Marnane, "Energy-Efficient Low Duty Cycle MAC Protocol for Wireless Body Area Networks," *IEEE Transactions-Information Technology in Biomedicine*, vol. 13, no. 6, pp. 915-925, November, 2009. Article (CrossRef Link)
[17] E.J. Kim, M. Kim, S. K. Youm, S. Choi and C. H. Kang, "Priority-based Service Differentiation Scheme for IEEE 802.15.4 Sensor Networks," *International Journal of Electronics and Communications*, vol. 61, no. 2, pp. 69-81, February, 2007. Article (CrossRef Link)
[18] Y. Zhang and G. Dolmans, "A New Priority-Guaranteed MAC Protocol for Emerging Body Area Networks," in *Proc. of 5th International Conference on Wireless and Mobile Communications (ICWMC '09)*, August, 2009. Article (CrossRef Link)
[19] K.A. Ali, J.H. Sarker and H.T. Mouftah, "QoS-based MAC Protocol for Medical Wireless Body Area Sensor Networks," in *Proc. of IEEE Symposium on Computers and Communications (ISCC2010)*, June, 2010. Article (CrossRef Link)
[20] K.S. Kwak and S. Ullah, "A traffic-adaptive MAC Protocol for WBAN," in *Proc. of 2010 IEEE-GLOBECOM Workshops (GC Wkshps)*, December, 2010. Article (CrossRef Link)
[21] D. Yun, S. Yoo, D. Kim, and D Kim, "OD-MAC: An On-Demand MAC Protocol for Body Sensor Networks based on IEEE 802.15.4," in *Proc. of 14th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'08)*, pp. 413-420, August, 2008. Article (CrossRef Link)
[22] H.M. Li and J.D. Tan, "An Ultra-Low-Power Medium Access Control protocol for Body Sensor Network," in *Proc. of 27th Annual International Conference of the Engineering in Medicine and Biology Society (IEEE-EMBS 2005)*, September, 2005. Article (CrossRef Link)
[23] C. Lee, H.S. Lee and S. Choi, "An Enhanced MAC Protocol of IEEE 802.15. 4 for Wireless Body Area Networks," in *Proc. of 5th International Conference of Computer Sciences and Convergence Information Technology (ICCIT)*, December, 2010. Article (CrossRef Link)
[24] B. Otgonchimeg and Y. Kwon, "Emergency Handling for MAC Protocol in Human Body Communication," *EURASIP Journal on Wireless Communications and Networking*, vol. 1, pp. 1-6, March, 2011. Article (CrossRef Link)
[25] Castalia : Simulator for Wireless Sensor Networks. Article (CrossRef Link)
[26] OMNeT++: Simulation Environment. Article (CrossRef Link)

Jay Shree Ranjit received B.E. degree in Computer Engineering from Kathmandu University, Dhulikhel, Nepal in 2006 and M.E. degree in Computer Engineering from Chosun University, Korea in 2013. His research interests include WBAN and WSN.

Subodh Pudasaini received B.E. in electrical and electronics engineering from Kathmandu University, Nepal, in 2005, and M.E. and PhD in computer engineering with concentration in wireless communications and networking from Chosun University, Korea, in 2008 and 2012, respectively. Currently he is a post-doctoral researcher at UWB Wireless Communications Research Center, Inha University, Korea. His research interests cover several areas of wireless networking technologies. He is particularly interested in the design, analytical modelling and empirical evaluation of the physical and link-layer protocols and algorithms for different wireless networks including WLANs, WPANs, and WBANs.

Seokjoo Shin received M.S. and Ph.D. degrees in information and communications from Gwangju Institute of Science and Technology (GIST), Korea, in 1999 and 2002, respectively. He joined the Mobile Telecommunication Research Laboratory, Electronics and Telecommunications Research Institute (ETRI), Korea, in 2002. In 2003, he joined the Faculty of Engineering, Chosun University, where he is currently a Full Professor in the Department of Computer Engineering. He spent 2009 as a Visiting Researcher at Georgia Tech, USA. His research interests include next-generation wireless communication systems and network security and privacy.